DEPARTMENT OF DEFENSE

DEFENSE INFORMATION SYSTEMS AGENCY

Joint Electronic Commerce Program Office (JECPO)
Electronic Commerce Engineering Division (JECE)
Evaluation and Demonstration Center (EDC)

Operational Procedures

EVALUATION AND DEMONSTRATION CENTER

Operational Procedures

Evaluation and Demonstration Center (EDC)
8725 John J. Kingman Road, Mail Stop 6205
Ft. Belvoir, VA 22060-6205
Phone (703) 767-0007 • Fax (703) 767-0695 DSN: 427

1. MANUAL OVERVIEW

1.1. INTRODUCTION

This manual was developed at the Joint Electronic Commerce Program Office (JECPO), Ft. Belvoir, VA. It is intended to be the basis and framework for control and management of the JECPO Evaluation and Demonstration Center (EDC).

1.2. PURPOSE

This manual establishes the foundation for general EDC control, utilization procedures, asset accountability, and resource management, as well as technical control and warehousing. It should facilitate an audit trail for management use, metrics collection, and highlights areas for future improvement and upgrade.

1.3. SCOPE

The procedures are brief and general in nature in order to retain their applicability throughout a wide range of changes and updates expected within the JECPO-EDC and functions. The procedures omit details that are unique or particular to a specific computer system, operating system (OS), application, or other software (SW). The procedures were designed for the individual Government or contractor manager assigned responsibility for the establishment, operation, and day-to-day control of the JECPO-EDC and the machines, equipment, software, and document designated as EDC assets. They also apply to the technical staff that plans to use the facilities. They are designed to be an aid and guide to all personnel in the efficient and responsible application of the overall JECPO process while using the EDC.

1.4. APPLICABILITY

The procedures herein are applicable to all personnel assigned to JECPO and any individual authorized JECPO laboratory access.

1.5. DOCUMENT UPDATES

Suggestions and recommendations for changes to, or amplification of, the procedures and guidelines contained in this manual are solicited from all JECPO managers and technical staff using the EDC. This document will reflect the mission, functions, and capabilities of the JECPO as it evolves. It will be periodically updated to ensure that it is consistent with the policies, processes, and procedures applicable within the JECPO-EDC environment.

2. JECPO-EDC OPERATIONS

2.1. INTRODUCTION

The JECPO vision for the EDC is to provide world class electronic business engineering evaluations and demonstration of the newest technology. EDC serves as the engineering agent for the Joint Electronic Commerce Program Office to accelerate the application of electronic business practices and technologies and prove next generation electronic business capabilities.

2.2. PURPOSE

The purpose for the EDC is to provide a state of the art facility for production, testing, and evaluation and demonstration of cutting-edge technology.

2.3. CUSTOMER

The EDC supports a wide range of customers. The following is a list of customers:

- Global Combat Support System (GCSS) customers are:
  -Single Procurement System-Defense Logistic Agency (DLA),
  -Electronic Document Access (EDA)-DLA,
  -Electronic Commerce (EC),
  -Electronic Data Interchange (EDI).

2.4. FACILITY OVERVIEW

See the EDC Lab layout.

3. LABORATORY DESIGN AND OPERATIONS

3.1. INTRODUCTION

The EDC houses a number of systems designed to support several programs. The systems are in a dynamic state of upgrade and evolution to meet the technical staff's needs and provide a standardized and stable environment to ensure maximum productivity.

3.2. MISSION

The JECOP-EDC mission is to provide a state-of-the-art facility for prototype development, testing, evaluation, and demonstration of current Electronic Commerce technology.

3.3. GOALS AND OBJECTIVE

The goal and objectives are to:

- Define, plan, and manage life-cycle support services for systems integration.
- Establish, manage, operate, and maintain EDC systems integration efforts to support best-of-breed selection and integration, network and site tuning, migration of commerce off-the-shell (COTS) / Government of-the-shell (GOTS) hardware and software systems and applications and operational systems support.
- Coordinate hardware and software procurement
- Provide systems administration supports
- Analyze emerging technologies and potential impact to EDC systems.

3.4. ARCHITECTURE

The two principal architecture are hardware and communications.

- Hardware: (Lab layout)

- Communication: (Communication Architecture)

4. COMPUTERS AND NETWORKING USE

4.1. POLICY

It is the policy of JECPO-EDC that use of computer and networking capability is primarily for evaluation and demonstration related purposed. All electronic transmissions and records, including email, computer files, web documents, etc., are consider JECPO-EDC's records and as such are subject to disclosure to JECPO-EDC management as well as to law enforcement, government officials, or to other third parties through the subpoena process.

4.2. SCOPE

This policy applies to all forms of computer and networking use, whether accessed on or from JECPO-EDC premises, accessed using JECPO-EDC computer equipment or via remote access methods. The scope includes the development and execution of computer codes, document processing and printing, electronic mail, database and file storage, World Wide Web access and development, and network access.

4.3. RESPONSIBILITIES

4.3.1. The EDC is responsible for managing the resources and for providing information to system users. The JECPO-EDC's staff are authorized by the Division Chief to monitor the use of the computational resources in order to ensure the appropriate use and that all applicable policies and standards of use and security are upheld. The JECPO-EDC's staff is further authorized to take appropriate measures in cases of breach of use and security policies. These measures are at the discretion of the EDC manager and designated System Administrators, and may include immediate disconnection of an offending system from the network, immediate revocation of a user account, and reporting the offending behavior to the Division Chief as appropriate. Further action, including legal action, is possible according to the nature of the offense and is at the discretion of the JECPO-EDC or DoD authorities.

4.3.2. The Webmaster oversees the contents of JECPO-EDC's web site. Webmasters have the responsibility of maintaining the quality, adhering to lab standards for web publishing, linking local topics with other divisions and agencies pages, and ensuring individuals posting content are familiar with DoD standards and policies. The webmasters are responsible for ensuring adherence to relevant security practices.

4.3.3. All Staff shall comply with the standards for use of computer and networking capability.

4.4. STANDARDS FOR USE OF COMPUTERS AND NETWORKING CAPABILITY

4.4.1. USER ACCOUNTS: All staff shall accept responsibility for any activity associated with their user account. The JECPO-EDC provides guidelines for account protection. As the security of all systems can be compromised with misuse, breaches shall be resolved immediately.

4.4.2. SOFTWARE PROTECTION: All stall are responsible for ensuring the laws for copyright, licensing and trademark protection are followed.

4.4.3. JECPO-EDC computers, portable electronic devices (PED), computing systems and its associated communication systems are to be used for official business of the EDC. Official business includes all authorized work connected with the research, design, testing, evaluation and demonstration.

4.4.4. Personal software, (e.g. personal holiday greeting card generators, or investment programs, etc.) shall not be placed on JECPO-EDC computers. Work of a personal nature shall not be generated during work time.

4.4.5. If engaging in a public professional forum, the user must differentiate personal opinions expressed by including a disclaimer to the effect that “the views expressed herein are solely the author’s and not those of JECPO-EDC or the U.S. Department of Defense.”

4.4.6. STANDARDS OF BEHAVIOR INCLUDE BUT ARE NOT LIMITED TO:

- Obscene, pornographic, offensive, threatening, harassing, or intimidating material shall not be entered into the computer or sent by electronic means.
- Computers shall not be used for any activity involving personal entertainment or financial gain (e.g. when operating and advertising a commercial enterprise or professional service on laboratory computer systems.)

5. BACKUP AND DISASTER POLICY

5.1. GENERAL OVERVIEW

The JECPO-EDC is committed to providing reliable and redundant backups of all system and user generated data on each of the systems, which it administers. The intent is not only to provide a service to the users who may wish to retrieve archived documents which are no longer stored on primary disk storage but also to prepare for both random mechanical disk failures as well as for the

recovery of JECPO-EDC work and research in the event of massive physical disaster (i.e. fire, flood, hurricane.)

5.2. SPECIFIC POLICY GUIDELINE – BACKUPS

5.2.1. Incremental backups are performed on a daily basis (Monday – Friday) on all user and system disks on all multi-user systems managed by the JECPO-EDC system administrators

5.2.2. Full disk backups (image / archive) are performed on a weekly basis for all disks.

5.2.3. Backup procedures are document in writing and updated on a regular basis, as changes are required. A copy of the current backup plans will be maintained in the JECPO-EDC Operations Guide.

5.2.4. Each backup procedure will generate a log file, which can be inspected on a daily basis to determine the success of failure of the backup.

5.2.5. There will be a primary and backup staff member assigned to perform the system backups for each system. Both the primary and backup staff member will inspect the backup log on a daily basis to verify the success of the backup and troubleshoot hardware and / or software problem related to the backup procedures.

5.3. BACKUP STORAGE

5.3.1. The daily backup tapes will be rotated on a biweekly basis. Daily incremental backups will be maintained for 10 days when they will be overwritten by the daily backup for two weeks.

5.3.2. Every Friday there will be an additional full system backup. Each of these system backups (image / archive) will be maintained for at least 5 weeks. The full system backup tape which is closed to the first for the month will be kept for 6 months.

5.4. DISASTER RECOVERY

5.4.1. The computer systems in EDC managed by the JECPO-EDC staff and located in DLA Headquarters Complex are included in a general insurance policy for buildings managed by the DLA Administration division.

5.4.2. The JECPO-EDC is protected by an automatic sprinkler system (water) and automatic power shut off at high tempurature. The DLA guards makes and daily inspection of this area during all off duty hours.

5.4.3. All JECPO-EDC machines are powered by an Uninterruptible Power System (UPS) which can maintain full power to all equipment for approximately 90 minutes.

6. PASSWORD RULES

6.1. PASSWORD SELECTION

6.1.1. Password contains at least eight non-blank characters, provided such passwords are allowed by the operating system or application.

6.1.2. Password contains a combination of letters (preferably a mixture of upper and lower case), numbers, and special characters, provided such passwords are allowed by the operating system or application.

6.1.3. Password contains a non-numeric in the first and last position.

6.1.4. Password does not contain the user ID.

6.1.5. Password does not include the user's own or, to the best of his/her knowledge, close friends – or relatives – names, employee serial number, Social Security number, birth date, phone number, or any information about him/her that the user believes could be readily learned or guessed.

6.1.6. Password does not, to the best of the user's knowledge, include common words that would be in an English dictionary, or from another language with which the user has familiarity.

6.1.7. Password does not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx".

6.1.8. Password does not, to the best of the user's knowledge, employ commonly used proper names, including the name of any fictional character or place.

6.2. PASSWORD PROTECTION

Individuals must not:

6.2.1. Share passwords; the only exception is “in emergency circumstances or when there is an overriding operational necessity”.

6.2.2. Leave clear-text passwords in a location inaccessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password;

6.2.3. Enable applications to retain passwords for subsequent re-use, this includes e-mail – do not let it remember your password.

6.3. PASSWORD CHANGING

Passwords must be changed:

- At least every 6 months.
- Immediately after sharing.
- As soon as possible, but within 1 business day after a password has been compromised, or after one suspects that a password has been compromised.
- On direction from management.
- EDC manager should be notified.

7. JECPO-EDC COMPUTER SECURITY GUIDELINES

7.1. PURPOSE

The computing and network infrastructure and equipment and the information and data residing on those systems are critical to the mission of the JECPO-EDC.

This policy statement has a twofold purpose. First, to emphasize to all JECPO-EDC staff and user community the importance of information system security and their role in its maintenance. The second purpose is to assign specific responsibilities for the provision of information and data security and for the security of the computing infrastructure itself.

7.2. SCOPE

The policy applies to all computational, storage, and network devices that make use of any of the JECPO-EDC resources. These include, but are not limited to, any system whether JECPO-EDC purchased or not, attached to the network, either directly or remotely by any means including any type of dial-up connection, or any other type of connection.

The policy applies to any and all users of the systems and resources. By attaching to any system, or making use of any JECPO-EDC computing or network resource the user implicitly agrees to this policy.

7.3. GOALS

The goals of these Security Guidelines are to provide a secure, robust, and useable computing environment for the working in JECPO-EDC. This goal embodies appropriate protection of data and resources from unauthorized used, protection from operational failures due to unauthorized use, and the use of procedures and policies that are effective without being operationally burdensome. Further goals are to ensure individual accountability for data, information, and other computing resources to which individuals have access, and to ensure that all applicable policies, directives, mandates, and legal requirements are applied and adhered to.

7.4. RESPONSIBILITIES

The following groups have responsibilities for implementing and maintaining the security goals set out in this policy.

7.4.1. JECPO-EDC staff: are responsible for informing users about this policy, and interacting with users on security issues. They are responsible for ensuring the continued operation of the systems and implementing appropriate security measures to comply with this security policy.

7.4.2. Local administrators, who include: Any user with super user (root) access to a UNIX or LINUX system, all WINDOWS NT domain or resource-domain administrators, are responsible for ensuring that the security of their systems is in accordance with this security policy.

7.4.3. End users: any person who has access to JECPO-EDC computing or network resource. They are responsible for using the resources in accordance with this policy, and for reporting any suspected breach of security to the JECPO-EDC manager or Division Chief.

7.5. ENFORCEMENT

The JECPO-EDC staff is authorized by Division Chief to take appropriate measures in cases of breach of use and security policies. These measures are at the discretion of the JECPO-EDC manager and system administrators, but may include immediate disconnection of a compromised system from the network, immediate blocking of a compromised user account, or any other measure deemed necessary. In addition, the use of any account or system in such a way that breaches this policy will be reported to the Division Chief or, if necessary, the DISA/DLA Security Specialist and may lead to further disciplinary and legal action.

7.6. GENERAL RESPONSIBILITIES

7.6.1. System Administrators are responsible for the maintenance and security of the computers and for following all applicable policies and procedures.

7.6.2. In order to prevent unauthorized access to data, software, and other resources residing on the network, all security mechanism of the system must be under exclusive control of the local administrator and relevant personnel of the JECPO-EDC.

7.6.3. In order to prevent the spread of malicious software and help enforce license agreements, users must ensure that software is properly licensed and safe.

7.6.4. Backups of all data residing on stand-alone systems and servers are the responsibility of the system administrators.

7.6.5. Each user is assigned a unique userid and password on receipt of a user account request and signed user agreement. Users must not share their assigned userid.

7.6.6. Use of traffic monitors / recorders, sniffers, routers, etc. is explicitly prohibited without the prior consent of the Division Chief.

7.7. SPECIFIC RESPONSIBILITIES

7.7.1. Users are expected to be familiar with JECPO-EDC security policies, and other policies, mandates and procedures. Users are responsible for their own behavior, specifically:

- Responsible for understanding and respecting relevant Federal laws, DoD policies and procedures, and other applicable security policies and associated practices for the JECPO-EDC computing environment.
- Responsible for employing available security mechanisms for protecting the confidentiality and integrity of their own information when required.
- Use file protection mechanism to maintain appropriate file access control. Select and maintain good passwords. Do not write passwords down, or disclose them to others.
- Use password share accounts. In general there are no shared accounts on central systems.
- Responsible for notifying JECPO-EDC manager, system administrators and the Division Chief if a security violation or failure is suspected or detected.
- Responsible for not exploiting system weaknesses.
- Do not intentionally modify, destroy, read, or transfer information in an unauthorized manner; do not intentionally deny others authorized access to or use of computing resources and information.
- Responsible for ensuring that backups of data and software on their own personal computer are performed.

- Responsible for being familiar with how malicious software (e.g. viruses) operates, methods by which it is introduced and spread, and vulnerabilities that are exploited by such software and unauthorized users.
- Responsible for knowing and utilizing appropriate procedures for the prevention, detection, and removal of malicious software.
- Users responsible for software materials brought into of the EDC for evaluation.

7.7.2. System Administrators are expected to utilize the available security services and mechanisms to support and enforce applicable security policies and procedures.

- Responsible for managing all users' access privileges to data, programs and functions.
- Responsible for monitoring all security related events and following up on any actual or suspected violations where appropriate. Responsible for notifying and coordinating with the JECPO-EDC manager, Division Chief and DISA/DLA Security Officers for investigation and monitoring of security related events.
- Responsible for maintaining and protecting system software and relevant files using available security mechanism and procedures. Specifically this includes applying any and all system patches as recommended or directly by DISA.
- Responsible for scanning local servers with anti-virus software at regular intervals to assure no virus becomes resident on the servers.
- Responsible for promptly notifying JECPO-EDC manager, Division Chief and DISA/DLA Security Officers of all computer security incidents, including malicious software:
    1. Notify the Computer Center if a penetration is in progress, assist other local administrators in responding to security violations.
    2. Cooperate with other local administrators and the Computer Center in finding violators and assisting in enforcement efforts.

- Responsible for providing assistance in determining the source of malicious software and the extent of contamination.
- Responsible for conducting timely audits of log files
- Responsible for backing up all data and software on the servers on a regular basis.
- Responsible conducting periodic reviews to ensure that proper security procedures are followed.
- Responsible for reporting all security incidents to the JECPO-EDC manager, Division Chief, and DISA/DLA Security Officers.